

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2004-520636

(P2004-520636A)

(43) 公表日 平成16年7月8日(2004.7.8)

(51) Int. Cl.⁷

G06F 11/00

G06F 13/00

F I

G06F 9/06

660N

G06F 13/00

351Z

テーマコード(参考)

5B076

5B089

審査請求 有 予備審査請求 有 (全 46 頁)

(21) 出願番号 特願2001-550634 (P2001-550634)
 (86) (22) 出願日 平成12年11月28日(2000.11.28)
 (85) 翻訳文提出日 平成14年6月28日(2002.6.28)
 (86) 国際出願番号 PCT/KR2000/001374
 (87) 国際公開番号 W02001/050344
 (87) 国際公開日 平成13年7月12日(2001.7.12)
 (31) 優先権主張番号 1999/68606
 (32) 優先日 平成11年12月31日(1999.12.31)
 (33) 優先権主張国 韓国(KR)
 (31) 優先権主張番号 2000/11282
 (32) 優先日 平成12年3月7日(2000.3.7)
 (33) 優先権主張国 韓国(KR)

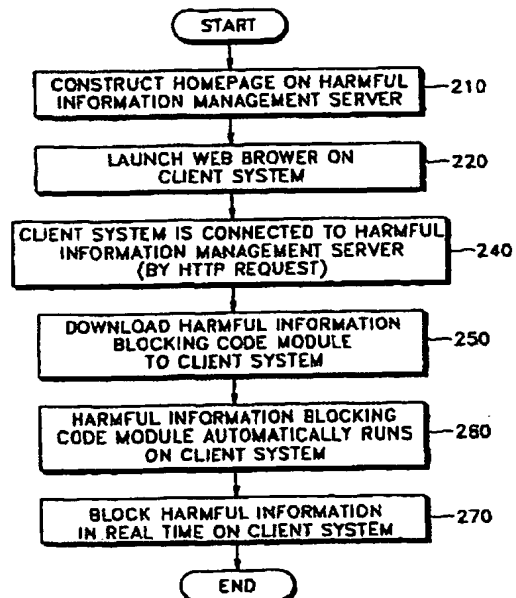
(71) 出願人 502234787
 インカインターネット カンパニー リミ
 テッド
 INCA INTERNET CO., L
 TD.
 大韓民国 152-053 ソウル クロ
 ーク クロー3ドン 197-7 エース
 テクノ タワー ザ セカンド 301
 (74) 代理人 100068755
 弁理士 恩田 博宣
 (74) 代理人 100105957
 弁理士 恩田 誠

最終頁に続く

(54) 【発明の名称】 オンライン上での有害情報遮断システム及び方法、並びにそのためのコンピュータで読出し可能な記録媒体

(57) 【要約】

ウェブサーバーとクライアントが相互連結されたコンピュータネットワークにおいて、オンラインでコンピュータウイルスなどの有害情報を診断、治療及び遮断するシステム及び方法を提供する。前記方法は、ウェブサーバーとクライアントシステムが相互連結されたコンピュータネットワークにおいて、前記ウェブサーバーがコンピュータネットワークを通じて前記クライアントシステムから接続要求を受信し、前記ウェブサーバーが前記クライアントシステムに有害情報遮断コードモジュールを送信し、前記有害情報遮断コードモジュールの伝送完了後、前記クライアントシステムにおいて前記有害情報遮断コードモジュールが自動的に実行され、コンピュータウイルスを含む有害情報をリアルタイムで遮断するものである。前記有害情報遮断コードモジュールは、ただ有害情報管理サーバーにオンラインで接続するだけで前記クライアントシステムに自動的に伝送及びインストールされるので、別途のインストールなしに便利にクライアントシステム上で検出された有害情報をリアルタイムで能動的に遮断することができる。



【特許請求の範囲】**【請求項1】**

コンピュータウイルスを含む有害情報を遮断する方法において、

(a) ウェブサーバーとクライアントシステムが相互連結されたコンピューターネットワークにおいて、前記ウェブサーバーがコンピューターネットワークを通じて前記クライアントシステムからの接続要請を受信するステップ；

(b) 前記ウェブサーバーが前記クライアントシステムに有害情報遮断コードモジュールを送信するステップ；及び

(c) 前記有害情報遮断コードモジュールの送信が完了すると、前記クライアントシステム上で前記有害情報遮断コードモジュールが自動的に駆動され、コンピュータウイルスを含む有害情報をリアルタイムで遮断するステップを含むことを特徴とする方法。

【請求項2】

前記ステップ(c)が、

(c1) 前記クライアントシステム上におけるファイル入出力(I/O)を監視するステップ；

(c2) 前記ステップ(c1)で監視されたファイルの有害有無を前記クライアントシステム上で判断するステップ；及び

(c3) 前記ステップ(c2)で有害と判断されたファイルの治療が可能な場合は適切な処理を行い、前記ステップ(c2)で有害と判断されたファイルの治療が不可能な場合は該当ファイルの実行を中止させるステップを含むことを特徴とする請求項1に記載の方法。

【請求項3】

前記ステップ(c3)において、

前記ウェブサーバーは、前記ステップ(c2)で有害と判断されたファイル関連情報の提供を受けることを特徴とする請求項2に記載の方法。

【請求項4】

前記ステップ(c3)において、

前記ステップ(c2)で有害と判断されたファイルを処理することができない

場合は、そのファイルを前記ウェブサーバーに伝送することを特徴とする請求項3に記載の方法。

【請求項5】

前記ステップ(c3)は、前記ステップ(c3)の実行に対し前記クライアントシステム利用者の承認を要請するステップを含むことを特徴とする請求項2に記載の方法。

【請求項6】

前記ステップ(c)は、

(c1) 前記クライアントシステム上におけるネットワークパケット入出力(I/O)を監視するステップ；

(c2) 前記ステップ(c1)で監視されたパケットの有害有無を前記クライアントシステム上で判断するステップ；及び

(c3) パケットが有害であると決定されれば、そのパケットI/Oに割り当てられた通信ポートを遮断するステップを含むことを特徴とする請求項1に記載の方法。

【請求項7】

前記ステップ(c)で実行された有害情報遮断コードモジュールが、クライアントシステム上で駆動中である現在のプロセスの有害有無を点検することを特徴とする請求項1に記載の方法。

【請求項8】

前記クライアントシステムが接続しようとするインターネットアドレスが、既に知られた有害サイトである場合は、前記ステップ(c)で実行された前記有害情報遮断コードモジュールが、その有害サイトへの接続を防止することを特徴とする請求項1に記載の方法。

【請求項9】

前記ステップ(c)で実行された有害情報遮断コードモジュールは、現在の有害情報遮断コードモジュールの駆動状態を別途のウィンドウに表示し、前記ウィンドウを閉じれば、前記有害情報遮断コードモジュールの実行が終了することを特徴とする請求項1に記載の方法。

【請求項10】

前記ステップ(c)で実行される有害情報遮断コードモジュールは、前記クライアントシステムが他のウェブサーバーに接続しようとする場合にも、前記クライアントシステム上でそのまま継続して動作することを特徴とする請求項1に記載の方法。

【請求項11】

前記ステップ(b)で伝送される有害情報遮断コードモジュールが、Active-XTMまたはJavaTMプログラムであることを特徴とする請求項1に記載の方法。

【請求項12】

前記有害情報遮断コードモジュールが、識別されたコンピュータウイルスとのパターン比較によって、確認されていないコンピュータウイルスを検出する機能を有することを特徴とする請求項1に記載の方法。

【請求項13】

コンピュータウイルスを含む有害情報を遮断する方法において、

(a) 第1ウェブサーバー、第2ウェブサーバー及びクライアントシステムが相互連結されたコンピューターネットワーク上において、前記クライアントシステムをコンピューターネットワークを通じて前記第2ウェブサーバーと連結するステップ；

(b) 前記第2ウェブサーバーから前記クライアントシステムに提供された情報に従って、コンピューターネットワーク上で前記クライアントシステムを前記第1ウェブサーバーと連結するステップ；

(c) 前記第1ウェブサーバーが前記クライアントシステムに有害情報遮断コードモジュールを伝送するステップ；及び

(d) 前記有害情報遮断コードモジュールの伝送が完了すると、前記クライアントシステムにおいて前記有害情報遮断コードモジュールが自動的に駆動され、コンピュータウイルスを含む有害情報をリアルタイムで遮断するステップを含むことを特徴とする方法。

【請求項14】

前記ステップ（d）が；

（d 1）前記クライアントシステム上におけるファイル入出力（I／O）を監視するステップ；

（d 2）前記クライアントシステムのステップ（d 1）で監視されたファイルの有害有無を前記クライアントシステムで判断するステップ；及び

（d 3）前記ステップ（d 2）で有害と判断されたファイルの治療が可能な場合は該当ファイルを適切に処理し、前記ステップ（d 2）で有害と判断されたファイルの治療が不可能な場合は該当ファイルの実行を中止させるステップを含むことを特徴とする請求項 1 3 に記載の方法。

【請求項 1 5】

前記ステップ（d）で実行された有害情報遮断コードモジュールは、前記クライアントシステムが他のウェブサーバーに接続しようとする場合にも、前記クライアントシステムにおいてそのまま継続して動作することを特徴とする請求項 1 3 に記載の方法。

【請求項 1 6】

コンピュータウイルスを含む有害情報を遮断するオンラインサービスの提供方法において、

（a）第 1 ウェブサーバーとクライアントシステムが相互連結されたコンピュータネットワーク上において、前記第 1 ウェブサーバーにオンラインサービスのためのホームページを構築するステップ；

（b）前記第 1 ウェブサーバーが、コンピュータネットワークを通じて前記クライアントシステムからの接続要請を受信するステップ；及び

（c）前記第 1 ウェブサーバーが前記クライアントシステムに有害情報遮断コードモジュールを伝送するステップを含み、

前記有害情報遮断コードモジュールが、前記クライアントシステム上で自動的に駆動されて、コンピュータウイルスを含む有害情報をリアルタイムで遮断することを特徴とする方法。

【請求項 1 7】

前記ステップ（b）において、前記第 1 ウェブサーバーが受信した接続要請は、

前記クライアントシステムが前記第1ウェブサーバーとは異なる第2ウェブサーバーに接続した後、前記第2ウェブサーバーから提供された情報に従って前記クライアントシステムで発生したものであることを特徴とする請求項16に記載の方法。

【請求項18】

前記ステップ(c)で伝送される有害情報遮断コードモジュールが、前記クライアントシステム上のファイル入出力(I/O)を監視することによってファイルの有害有無を判断し、有害なものと判定されたファイルの処理が可能な場合は処理を行い、有害なものと判定されたファイルの処理が不可能な場合はファイルの実行を中止させることを特徴とする請求項16に記載の方法。

【請求項19】

前記ステップ(c)で伝送される前記有害情報遮断コードモジュールは、前記クライアントシステムが他のウェブサーバーに接続しようとする場合にも、前記クライアントシステム上においてそのまま継続して駆動することを特徴とする請求項16に記載の方法。

【請求項20】

コンピュータウイルスを含む有害情報を遮断するシステムにおいて、
コンピューターネットワークを通じてオンラインサービスを提供する第1ウェブサーバーと、
前記コンピューターネットワークを通じて前記第1ウェブサーバーと相互連結されたクライアントコンピュータとを含み、
前記クライアントコンピュータが前記コンピューターネットワークを通じて前記第1ウェブサーバーに接続すると、前記第1ウェブサーバーは前記クライアントコンピュータに有害情報遮断コードモジュールを伝送し、前記有害情報遮断コードモジュールは、前記クライアントシステム上で自動的に実行されて、コンピュータウイルスを含む有害情報をリアルタイムで遮断することを特徴とするシステム。

【請求項21】

前記有害情報遮断コードモジュールが、前記クライアントシステム上のファイル

入出力（I/O）を監視することによってファイルの有害有無を判断し、有害であると判定されたファイルが処理可能であれば処理を行い、有害であると判定されたファイルの処理が不可能であればファイルの実行を中断させることを特徴とする請求項20に記載のシステム。

【請求項22】

前記有害情報遮断コードモジュールは、現在の有害情報遮断コードモジュールの実行状態を別途のウィンドウに表示し、前記ウィンドウを閉じれば、前記有害情報遮断コードモジュールの実行が終了することを特徴とする請求項20に記載のシステム。

【請求項23】

前記クライアントコンピュータと前記コンピューターネットワークを通じて相互連結され、前記コンピューターネットワークを通じてオンラインサービスを提供する第2ウェブサーバーをさらに含み、

前記クライアントコンピュータが前記コンピューターネットワークを通じて前記第2ウェブサーバーに接続した場合、前記第2ウェブサーバーは前記クライアントコンピュータに前記第1ウェブサーバーへの接続に用いられたハイパーリンク情報を提供することを特徴とする請求項20に記載のシステム。

【請求項24】

前記有害情報遮断コードモジュールは、前記クライアントコンピュータが他のウェブサーバーに接続しようとする場合にも、前記クライアントコンピュータにおいてそのまま継続して動作することを特徴とする請求項20に記載のシステム。

【請求項25】

有害情報を遮断するコンピュータプログラムが記録されているコンピュータで読出すことのできる記録媒体において、前記コンピュータプログラムは、コンピューターネットワークを通じてウェブサーバーからクライアントシステムに伝送されて、前記クライアントシステム上で自動的に実行され、

前記有害情報を遮断する方法は、；

（a）前記クライアントシステムにおけるファイル入出力（I/O）を監視するステップ；

(b) 前記ステップ(a)で監視されたファイルの有害有無を前記クライアントシステムで判断するステップ；

(c) 前記ステップ(b)で有害と判断されたファイルの処理が可能な場合は適切な処理を行い、前記ステップ(b)で有害と判断されたファイルの処理が不可能な場合はファイルの実行を中止させるステップ；及び

(d) 前記ステップ(b)で有害と判断されたファイル関連情報を前記ウェブサーバーに提供するステップを含むことを特徴とするコンピュータで読出し可能な記録媒体。

【請求項26】

前記ステップ(d)において、ステップ(b)で有害と判定されたファイルの処理が不可能であれば、前記有害ファイルを前記ウェブサーバーに伝送することを特徴とする請求項25に記載のコンピュータで読出し可能な記録媒体。

【発明の詳細な説明】**(技術分野)**

本発明は、保安システムに関するもので、特にクライアントとウェブサーバーが連結されたコンピューターネットワークにおいて、オンラインでコンピュータウイルスなどの有害情報を診断、治療及び遮断するシステム及び方法に関するものである。

【0001】**(背景技術)**

コンピューターネットワーク関連技術、特にワールドワイドウェブ（以下“ウェブ”という）技術の発達に伴って、コンピューターネットワーク上の利用者、特にインターネットの利用者数が急速に増加している。今やインターネットはもはや仮想空間における新しい技術またはサービスの領域ではなく、実生活の一部として深く根を下ろしつつある。ショッピング、競売、金融、広告などの営業分野がインターネットを軸として設立されている。また、コンピュータの利用者はインターネットで各種情報を得たり、多様な経済活動を手軽に行っている。

【0002】

インターネットは、その利用者に多様な便利さを提供している。しかしその反面、コンピューターネットワークを通じた個人情報の不法流出または各種コンピュータウイルスなどの新しい危険要素が、コンピュータ及びインターネット関連技術の発達と共に急速に増加している。コンピュータウイルスなどの有害情報による弊害は深刻である。報道によると、1999年上半期におけるコンピュータウイルスによる全世界の被害額は76億ドルで、これは1998年の年間の被害額である25億ドルの3倍強であると報告されている。

【0003】

例えば、CIH (Chernobyl) ウイルスのような悪性コンピュータウイルスはハードディスクの内容全体を消してしまうほどの破壊力を持ち、韓国をはじめとする全世界のあちこちに甚だしい被害をもたらした。最近では、コンピュータウイルスと共にコンピュータを遠隔調整することのできる‘スパイ’ファイルであるバックオリフィス (back orifice)、スクールバス (sc

h o o l b u s) などのような新種の有害情報が、インターネットを通じてコンピュータに浸透し、そのコンピュータから個人情報不法に流出している。

【0004】

このような各種有害情報に対する従来の対処方法としては、基本的に先被害／後復旧方式であった。このような保護政策は、コンピュータシステムが識別されていない有害情報によって被害を被ってから初めてその対処方案（例えば、ワクチンプログラムの開発）を模索する手動的な方式である。このような保護政策における他の短所は、有害情報に対処するための各種ワクチンプログラムなどを各パーソナルコンピュータに手動でインストールしなければならないということであり、コンピュータ利用者には煩わしさがあった。さらに、各種有害情報は絶えず新しく考案されてインターネットを通じて速いスピードで配布されているため、常に最新バージョンのワクチンプログラムを備えるのは容易なことではない。

【0005】

したがって、現在インストールされているワクチンプログラムでは対処できない新しいコンピュータウイルスのような新種有害情報が利用者のコンピュータシステムに浸透した場合は、これを遮断する方法がなく、このような新種コンピュータウイルス等によるコンピュータシステムの機能麻痺または個人情報の流出被害は回避不可能なものと認識されている。また、コンピュータ利用者は、確認されていないコンピュータウイルスが発見される度に、最新バージョンのワクチンプログラムを確保するために、有害情報関連専門業者またはオンライン通信会社にアクセスしなければならなかった。しかも、このような最新バージョンのワクチンプログラムをダウンロードした後、手動でインストールしなければならないため、無駄な時間が費やされるという煩わしさがあった。

【0006】

また、従来の有害情報からコンピュータを保護する方式では、有害情報の発生またはこれによる被害を有害情報関連専門業者に効率的に報告する通信チャンネルが存在しなかったため、有害情報関連専門業者が有害情報の分布及び被害状況に関する体系的な情報分析及び統計資料を構築する方法がなかった。

【0007】

(発明の開示)

本発明は上記問題点に鑑みてなされたものであり、クライアントシステムがコンピュータネットワークを通じてウェブサーバーに接続することで、前記クライアントシステムに有害情報遮断プログラムが自動的に伝送及びインストールされ、クライアントシステムのファイル及び通信パケットの入出力をリアルタイムで監視し、有害情報を能動的に遮断できるオンライン有害情報遮断システム及び方法を提供することを第1の目的とする。

【0008】

本発明は、コンピュータネットワーク上のウェブサーバーでオンライン有害情報遮断サービスを提供する方法を提供することを第2の目的とする。

本発明は、前記有害情報遮断プログラムが保存されているコンピュータで読み出すことのできる記録媒体を提供することを第3の目的とする。

【0009】

上記第1の目的を達成するために、本発明はコンピュータウイルスを含む有害情報を遮断する方法において、(a) ウェブサーバーとクライアントシステムが相互連結されたコンピュータネットワークにおいて、前記ウェブサーバーがコンピュータネットワークを通じて前記クライアントシステムからの接続要請を受信するステップ；(b) 前記ウェブサーバーが前記クライアントシステムに有害情報遮断コードモジュールを伝送するステップ；及び(c) 前記有害情報遮断コードモジュールの伝送完了後、前記クライアントシステムにおいて前記有害情報遮断コードモジュールが自動的に実行され、コンピュータウイルスを含む有害情報をリアルタイムで遮断するステップを含むことを特徴とする。

【0010】

前記ステップ(c)は、(c1) 前記クライアントシステム上におけるファイル入出力を監視するステップ；(c2) 前記クライアントシステム上において前記ステップ(c1)で検索されたファイルの有害有無を判断するステップ；及び(c3) 前記ステップ(c2)で有害と判断されたファイルの治療が可能な場合は該当ファイルを適切に処理し、前記ステップ(c2)で有害と判断されたファイルの治療が不可能な場合は該当ファイルの実行を中止させるステップが含まれ

る。前記ステップ(c3)において、前記ウェブサーバーは前記ステップ(c2)で有害と判断されたファイル関連情報の提供を受ける。

【0011】

また、前記ステップ(c)は、(c1)前記クライアントシステム上におけるネットワークパケット入出力を監視するステップ；(c2)前記クライアントシステム上において前記ステップ(c1)で検索されたパケットの有害有無を判断するステップ；及び(c3)いずれか1つのパケットが有害であると決定された場合、そのパケットの入出力に割り当てられた通信ポートを遮断するステップをさらに含んでいる。

【0012】

前記ステップ(c)で実行された有害情報遮断コードモジュールは、現在の有害情報遮断コードモジュールの実行状態を別途のウィンドウに表示し、前記ウィンドウを閉じれば、前記有害情報遮断コードモジュールの実行が終了されることが好ましい。前記ステップ(c)で実行される有害情報遮断コードモジュールは、前記クライアントシステムが他のウェブサーバーに接続しようとする場合にも、前記クライアントシステムでそのまま継続して動作することが好ましい。前記ステップ(b)で伝送される有害情報遮断コードモジュールは、Active-X™またはJava™プログラムであることが好ましい。

【0013】

他の実施形態として、本発明は、コンピュータウイルスを含む有害情報を遮断する方法において、(a)第1ウェブサーバー、第2ウェブサーバー及びクライアントシステムが相互連結されたコンピューターネットワークにおいて、前記クライアントシステムがコンピューターネットワークを通じて前記第2ウェブサーバーに接続するステップ；(b)前記第2ウェブサーバーから前記クライアントシステムに提供された情報に従って、前記クライアントシステムがコンピューターネットワークを通じて前記第1ウェブサーバーに接続するステップ；(c)前記第1ウェブサーバーが前記クライアントシステムに有害情報遮断コードモジュールを伝送するステップ；及び(d)前記有害情報遮断コードモジュールの伝送完了後、前記クライアントシステムにおいて前記有害情報遮断コードモジュールが

自動的に実行され、コンピュータウイルスを含む有害情報をリアルタイムで遮断するステップを含む。

【0014】

また本発明の第2の目的は、コンピュータウイルスを含む有害情報を遮断する方法を提供するオンラインサービスにより達成されるが、前記方法は、(a) 第1ウェブサーバーとクライアントシステムが相互連結されたコンピューターネットワークにおいて、前記第1ウェブサーバーにオンラインサービスのためのホームページを構築するステップ；(b) 前記第1ウェブサーバーがコンピューターネットワークを通じて前記クライアントシステムからの接続要請を受信するステップ；及び(c) 前記第1ウェブサーバーが前記クライアントシステムに有害情報遮断コードモジュールを伝送し、前記有害情報遮断コードモジュールが前記クライアントシステムにおいて自動的に実行されて、コンピュータウイルスを含む有害情報をリアルタイムで遮断するステップを含む。

【0015】

前記ステップ(b)において、前記第1ウェブサーバーが受信した接続要請は、前記クライアントシステムが前記第1ウェブサーバーとは異なるウェブサーバーである第2ウェブサーバーに接続した後、前記第2ウェブサーバーから提供された情報に従って前記クライアントシステムが前記第1ウェブサーバーに要請したものであってもよい。

【0016】

また本発明の第1の目的は、コンピュータウイルスを含む有害情報を遮断するシステムにより達成されるが、前記システムは、コンピューターネットワークを通じてオンラインサービスを提供する第1ウェブサーバーと、前記コンピューターネットワークを通じて前記第1ウェブサーバーと連結されたクライアントコンピュータとを含み、前記クライアントコンピュータが前記コンピューターネットワークを通じて前記第1ウェブサーバーに接続すると、前記第1ウェブサーバーは前記クライアントコンピュータに有害情報遮断コードモジュールを伝送し、前記有害情報遮断コードモジュールは、前記クライアントコンピュータにおいて自動的に実行されて、前記クライアントコンピュータでコンピュータウイルスを含む

有害情報をリアルタイムで遮断することを特徴とする。

【0017】

前記有害情報遮断システムは、コンピューターネットワークを通じて前記クライアントコンピュータと連結され、コンピューターネットワークを通じてオンラインサービスを提供する第2ウェブサーバーをさらに含み、前記クライアントコンピュータがコンピューターネットワークを通じて前記第2ウェブサーバーに接続した場合、前記第2ウェブサーバーは、前記クライアントコンピュータに前記第1ウェブサーバーに接続するのに用いられるハイパーリンク情報を提供することが好ましい。

【0018】

また本発明の第3の目的は、有害情報を遮断するコンピュータプログラムが記録されているコンピュータで読出すことのできる記録媒体により達成されるが、前記コンピュータプログラムは、コンピューターネットワークを通じてウェブサーバーからクライアントシステムに伝送され、前記クライアントシステムにおいて自動的に実行され、前記有害情報の遮断は、；(a) 前記クライアントシステムにおけるファイル入出力を監視するステップ；(b) 前記クライアントシステムにおいて前記ステップ(a)で監視されたファイルの有害有無を判断するステップ；(c) 前記ステップ(b)で有害と判断されたファイルの治療が可能な場合は該当ファイルを適切に処理し、前記ステップ(b)で有害と判断されたファイルの治療が不可能な場合は該当ファイルの実行を中止させるステップ；及び

(d) 前記ステップ(b)で有害と判断されたファイル関連情報を前記ウェブサーバーに通知するステップ含む。

【0019】

(発明を実施するための最良の形態)

図1aは、本発明の実施形態が適用されるシステム構成図を概略的に示したものであり、ウェブサーバーの有害情報管理サーバー110はホームページを備えており、インターネットなどのコンピューターネットワークを通じてクライアントコンピュータ130と連結されている。

【0020】

有害情報管理サーバー110は、クライアントコンピュータ130において有害情報をリアルタイムで遮断できる有害情報遮断コードモジュールを提供するオンラインサービスを提供する。ここで、「有害情報」とは、コンピュータシステム及び／またはコンピュータネットワークに悪影響を引き起こす好ましくないオブジェクトまたは行為を総称する用語であり、コンピュータウイルス、個人情報の不法流出及びインターネット上の猥褻サイトなどが含まれる。

【0021】

図2aは、図1aに示したシステムの動作について説明している。本発明によるオンライン有害情報遮断方法の第1実施形態を図2aを参考にしながら説明する。

【0022】

先ず、有害情報管理サーバー110は、オンラインサービスを提供するためにホームページを構築する(ステップ210)。コンピュータ利用者は、クライアントコンピュータ130(以下、単に‘クライアント’という)でウェブブラウザを駆動する(ステップ220)。クライアント130が前記有害情報管理サーバー110に接続すると(ステップ240)、有害情報管理サーバー110はクライアント130に有害情報遮断コードモジュールを伝送する(ステップ250)。

【0023】

ここで、クライアント130と有害情報管理サーバー110との接続は、ハイパーテキスト伝送プロトコル(Hyper Text Transfer Protocol)のフォーマットされた要請(HTTP request)によって、また有害情報管理サーバー110からクライアント130への有害情報遮断コードモジュールの伝送は、HTTP応答(HTTP response)によって行われる。一般的にHTTP要請は、ウェブブラウザにおいて有害情報管理サーバー110のURL(Universal Resource Locator)を入力したり、該当URLリンクをクリックする通常的な方式で行われる。

【0024】

適切には、有害情報遮断コードモジュールは、クライアント130で駆動される

実行可能なアプリケーションプログラムである。例えば、マイクロソフト社のウィンドウ環境における使用のためのActive X™制御、及びウェブブラウザで実行され得るジャバアプレット（Java™ applet）及びジャバスクリプト（JavaScript™）がある。また、高級言語で作成され、オブジェクトコード化されたプログラムをウェブブラウザとリンクさせて、該当プログラムを実行させてもよい。

【0025】

また、有害情報遮断コードモジュールは、ユーザーインターフェースのために提供された別途のウィンドウと関連して実行されるが、現在の有害情報遮断コードモジュールの実行状態をそのウィンドウに表示することが好ましい。この方法において、有害情報管理サーバー110にクライアント130が接続すれば、先ず別途のウィンドウを開設できるHTTP応答をクライアントに提供し、別途のウィンドウを通じて行われたクライアント130からのHTTP要請に対するHTTP応答として有害情報遮断コードモジュールを提供することが好ましい。前記ウィンドウを閉じれば、前記有害情報遮断コードモジュールの実行が中止される。前記ユーザーインターフェースのための別途のウィンドウは、有害情報遮断コードモジュールの実行状態情報の表示用途以外にも多様に活用でき、例えば各種ニュースまたはバナー広告などを掲載することもできる。

【0026】

前記有害情報遮断コードモジュールの伝送が完了すると、前記有害情報遮断コードモジュールはクライアント130において自動的に実行され（ステップ260）、コンピュータウイルスを含む有害情報をリアルタイムで遮断する（ステップ270）。有害情報遮断コードモジュールは、クライアント130においてリアルタイムで動作するため、ウィンドウが閉じられない限り、クライアント130が異なるウェブサーバーに接続しようとする場合でも、クライアント130において駆動を続ける。したがって、クライアント130は、有害情報管理サーバー110への一回の接続によって、自分のコンピュータのための有害情報遮断サービスの提供をリアルタイムで受けることができる。

【0027】

有害情報遮断コードモジュールのメカニズムを説明する前に、図1 aを参考にしながら説明した前記実施形態の変形例（以下、第2実施形態）を説明する。図1 bは本発明による第2実施形態が適用されるシステム構成図を説明し、図2 bは本発明によるオンライン有害情報遮断方法の第2実施形態を説明するフローチャートである。

【0028】

図1 bに示すように、前記システムは、前記有害情報管理サーバー110の他にネットワーク上でオンラインサービスを提供するウェブサーバー120（以下‘第2ウェブサーバー’という。）をさらに含む。前記第2ウェブサーバー120は、インターネットなどのコンピューターネットワークを通じてクライアントシステムと連結されている通常的なウェブサーバーである。

【0029】

この実施形態において、図2 bを参考にすると、ステップ210及びステップ220が、図2 aを参考にして説明した前記第1実施形態においてのような方法で行われる。次いで、クライアント130が主に前記第2ウェブサーバー120にアクセスする（ステップ230）。

【0030】

前記第2ウェブサーバー120は、自分が提供するオンラインサービス情報の他に、有害情報管理サーバー110への接続に用いられるハイパーリンク（hyperlink）情報をクライアント130に提供する（ステップ235）。前記ハイパーリンク情報は、有害情報管理サーバー110のフロントホームページ用リンク情報ではなく、クライアント130が別途のウィンドウを通じて前記有害情報管理サーバー110から有害情報遮断コードモジュールを直接受信することができるようにするリンク情報であることが好ましい。

【0031】

次に、クライアント130は、第2ウェブサーバー120からの前記ハイパーリンク情報に従って、有害情報管理サーバー110にHTTP要請を提供する（ステップ245）。前記有害情報管理サーバー110は、前記クライアント130からの前記HTTP要請に対するHTTP応答として有害情報遮断コードモジュ

ールを伝送する（ステップ255）。

【0032】

有害情報遮断コードモジュールの伝送が完了すると、前記有害情報遮断コードモジュールはクライアント130において自動的に実行され（ステップ260）、コンピュータウイルスを含む有害情報をリアルタイムで遮断する（ステップ270）、というのは第1実施形態におけると同様である。

【0033】

前記有害情報遮断コードモジュールについてより詳しく説明する。図3は、本発明に適用される有害情報遮断コードモジュールの一例の構成を示し、図4は、図3に示した有害情報遮断コードモジュールの動作を説明するフローチャートである。

【0034】

図3に示すように、有害情報遮断コードモジュールは、入出力管理ユニット310、有害情報遮断ユニット320及び情報伝達ユニット330を含む。また、有害情報遮断コードモジュールは、現在の有害情報遮断コードモジュールの実行状態を表示する別途のウィンドウ340と関連し、前記ウィンドウ340を閉じれば、有害情報遮断コードモジュールの実行が終了されるのが好ましいというのは上述のとおりである。

【0035】

前記入出力管理部310は、クライアント130上におけるファイル入出力（I/O）を監視する。前記ファイルI/Oの監視とは、ファイルI/Oルーチンを奪って（hooking up）該当ファイル情報を得ることを意味する。前記入出力管理ユニット310は、ネットワークからの有害情報を遮断するために、クライアント130上におけるネットワークパケットI/Oも監視することが好ましい。バックオリフィスウイルスと不法個人情報流出させることの可能なコンピュータウイルスは、ファイルI/Oを点検したり、プロセスを点検することによって遮断されもするが、その内容は後述する。適切には、入出力管理ユニット310は、クライアント130が接続しようとするインターネットアドレスをモニターする機能も持っているため、コンピュータ利用者が猥褻サイトに接続す

ることを遮断する。

【0036】

有害情報遮断ユニット320は、ファイルまたはパケットの有害有無を診断し、そのファイルまたはパケットが有害である場合は、適切な治療を行う。情報伝達ユニット330は、有害情報であると判断されたファイルまたはパケットの情報を有害情報管理サーバー110に通知する。

【0037】

図4を参照しながら前記有害情報遮断コードモジュールの動作を説明すると、前記クライアント130で自動的に実行される有害情報遮断コードモジュールは、一次的に現在クライアント130で駆動中であるプロセスの有害有無を点検する（ステップ410）。これは、現在メモリに搭載されて実行中であるプロセスは、今後実行される全てのプロセスに影響を与え得るためである。また、バックオフィスのような不法個人情報流出ウイルスは、プロセス形態で動作しながら、外部のコンピュータシステムを通じて利用者コンピュータを遠隔制御することができるためである。

【0038】

プロセスの有害有無を点検する1つの方法は、メモリにロードされている進行中のプロセスの目録を作成し、各プロセスに対応するファイルの有害有無を判断することである。もし該当ファイルが有害であると判断された場合は、該当プロセスを有害プロセスと判断し、該当プロセスを中断させる。該当有害ファイルに対しても適切な処理を行うことが好ましい。また、有害情報遮断コードモジュールは、有害情報を診断した後、適切な処理を行う前に使用者に前記有害情報の存在を通知し、治療実行に対して利用者の承認を求めることが好ましい。

【0039】

次に、クライアント130上における全てのファイル入出力を監視する（ステップ420）。上述したとおり、前記ファイルI/Oの監視は、ファイルI/Oルーチンを途中で奪う方式で行われる。例えば、ウィンドウ環境におけるI/OルーチンであるVxDの実行を奪うことにより監視を行う。

【0040】

ステップ420で、ネットワークからの有害情報の浸透を防ぐために、前記ファイルI/Oと共にネットワークパケットI/Oを監視することが好ましいのは上述のとおりである。ネットワークパケットI/Oの監視は、ソケットI/Oルーチン（ウィンドウ環境では“winsock”モジュールと呼ばれる）を奪うことにより行われることもある。

【0041】

また上述のとおり、ステップ420で、クライアント130が接続しようとするインターネットアドレスも監視し、好ましくない猥褻サイトへの接続を遮断する。このような好ましくない接続を防止するための監視は、HTTP要請メッセージまたはドメイン名サービス（DNS）のルックアップメッセージのヘッダを検査することにより行うことができる。

【0042】

言い換えれば、ステップ420は、クライアント130で発生する多様な有害情報を監視する追加機能を含むこともできる。前記有害情報遮断コードモジュールの次の動作をファイルI/Oの監視を参考にして説明する。しかし、ファイルI/Oの監視は、単に一例であるだけで、本発明がこれに制限されるものではない。

【0043】

次に、ステップ420で監視されたファイルの有害有無を判断する（ステップ430）。この判断は、有害情報の種類によって、またはアプリケーションの必要性によって多様な技法で行われる。例えば、既に知られているコンピュータウイルスのような有害情報とのパターン比較を行う方式が用いられ得る。一般的にコンピュータウイルスは一定の動作パターンを持っているため、ウイルスパターン比較方式は新種ウイルスを診断する1つのツールとなる。

【0044】

ステップ430で、ネットワークパケットが有害であるか否か、またはクライアント130が猥褻ウェブサイトに接続しようとしているか否かを判断するのが好ましい。

【0045】

監視された情報が安全であると判断されると、有害情報遮断コードモジュールは、そのファイルに対して何らの動作を行わない。したがって、利用者は有害情報遮断コードモジュールとは関係なく自分の作業をそのまま続けて行うことができる。

【0046】

監視された情報が有害であると判断されると、その監視された情報がファイルI/Oと関連したものであるか、またはパケットI/Oと関連したものであるかを決定し、その有害ファイルまたはパケットに対して適切な処理を行う。図4には示していないが、猥褻サイトアドレス遮断の場合は、クライアント130に健全なウェブサイトへHTTP要請メッセージを変更する方式が適用される。

【0047】

前記監視された情報がファイルI/Oと関連している場合は、その有害ファイルが適切に処理され得るかを判断する(ステップ450)。処理が可能であれば、その関連したファイル进行处理する(ステップ454)。もし処理が不可能であれば、該当ファイルの実行のみを中断させる(ステップ452)。ステップ454において、利用者に有害情報が検索されたことを通知し、その有害情報に対する処理を行うことに対して承認を要請する。

【0048】

最後に、もし有害情報を示す情報がオンライン上でクライアント130から検索された場合は、有害情報遮断コードモジュールを利用して前記有害情報管理サーバー110に通知することが好ましい(ステップ470)。もし前記検索された情報が新しい種類の有害情報であって処理が不可能である場合は、その識別されなかった有害情報と関連したファイル全体を有害情報管理サーバー110に伝送することが好ましい。もちろん、有害情報検出及び／または前記識別されなかった有害情報ファイルを有害情報管理サーバー110に伝送することに対し利用者の事前承認を求めることが好ましい。

【0049】

言い換えれば、この実施形態は、クライアント130で発生した有害情報を有害情報管理サーバー110に自動通知する機能を提供する。したがって、有害情報

管理サーバー110は、有害情報関連統計資料が得られるので、新種のコンピュータウイルスの出現に対し迅速な対処方案（例えばワクチン開発）を講ずることができる。このような方式で、有害情報管理サーバー110はクライアント130からの新種の有害情報を分析して適切な処理プログラムを開発し、最新の有害情報遮断コードモジュールを通じて前記クライアント130を攻撃する有害な情報を防ぐ適切な保安サービスを提供する。したがって、本発明は、オープンネットワーク環境で作動する利用者のコンピュータを各種有害情報による被害から保護することができる。

【0050】

この実施形態において、有害情報遮断コードモジュールによる有害情報の有害情報管理サーバー110への自動通知のための通信チャンネルは、例えば、SMTP（Simple Mail Transfer Protocol）またはFTP（File Transfer Protocol）などのインターネットメール伝送プロトコルを通じて具現することができる。より好ましくは、前記有害情報伝送のための別途の固有通信チャンネルを用いることが好ましい。

【0051】

これに対し、ステップ440において有害情報がパケットI/Oと関連したものと判定された場合は、そのパケットI/Oに割り当てられた通信ポートを遮断する（ステップ460）。もし通信チャンネルを通じた前記ネットワークパケットI/Oを支援する内部プロセスが存在する場合は、これを中断させることが好ましい。

【0052】

次に、通信ポートから浸透する有害情報に対する適切な処理は、ファイルI/Oと関連した有害情報に対する処理と類似している（ステップ462）。ステップ470で、前記有害情報管理サーバー110は、ネットワークパケットI/Oから前記有害情報の検出を通知される。

【0053】

これらの実施形態は、コンピュータで読出し可能なプログラムコードとして具現されてもよい。本発明は、コンピュータで読出すことのできる記録媒体からプロ

グラムを駆動させ、汎用デジタルコンピューターで行われるが、このような記録媒体にはマグネチック記録媒体（例えば、ROM、フロッピーディスク、ハードディスク等）、光学読出し媒体（例えば、CD-ROM、DVD等）及びキャリアウェーブ（例えば、インターネットを通じた伝送）のような媒体が含まれ、これに制限されるものではない。

【0054】

以上、本発明についてその好ましい実施形態を中心に検討した。本発明が属する技術の分野における通常の知識を有する者が、本発明の本質的な特性から逸脱しない範囲で変形された形態によって具現可能であることが理解できるであろう。したがって、この開示された実施形態は、限定的な観点ではなく説明的な観点から考慮されなければならない。本発明の範囲は、上述した説明にではなく特許請求の範囲に示されており、これと同等な範囲内にある全ての差は本発明に含まれるものと解釈されるべきである。

【0055】

（産業上の利用可能性）

上述したとおり、本発明によれば、ただ有害情報管理サーバーにオンラインで接続するだけで、有害情報遮断コードモジュールがクライアントシステムに自動的にインストールされるので、別途に手動でインストールしなくても、便利にクライアントシステムで発生する有害情報をリアルタイムで能動的に検出することができる。

【0056】

前記有害情報遮断コードモジュールは、クライアントシステムで検出された識別されなかったコンピュータウイルスが示す情報を前記有害情報管理サーバーに通知する機能を有する。したがって、有害情報管理サーバーは、有害情報に関する有用な統計的データを得ることができ、利用者のコンピュータに最新の保安サービスを提供するための有害情報遮断コードモジュールの最新配布版を継続してアップデートすることができる。

【0057】

また、有害情報遮断コードモジュールは、ネットワークパケット I/O の監視を

行うことができるが、これは、インターネットを通じた安全な電子商取引を保障する。特に、企業及び政府の主要機関のために、本発明は能動的にビジネス情報を保護したり、各種有害情報から国家保安と関連した機密情報なども能動的に守ることができるため、経済的な付加価値以外にも安保的な効果も達成することができる。

【図面の簡単な説明】

【図1 a】本発明の実施形態が適用される概略的なシステム構成図。

【図1 b】本発明の実施形態が適用される概略的なシステム構成図。

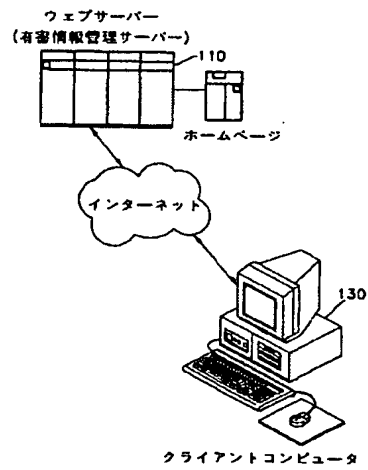
【図2 a】本発明によるオンライン有害情報遮断方法の適切な実施形態を説明するフローチャート。

【図2 b】本発明によるオンライン有害情報遮断方法の適切な実施形態を説明するフローチャート。

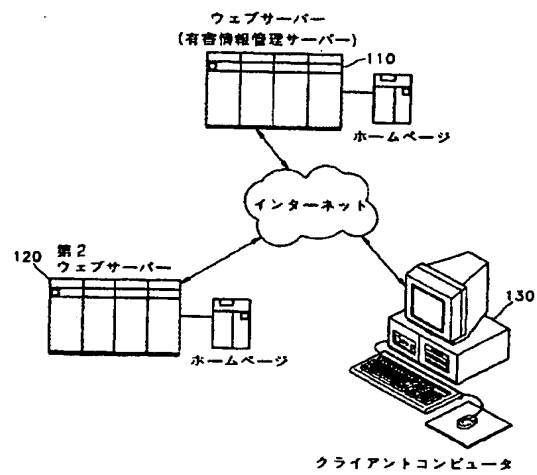
【図3】本発明に適用される有害情報遮断コードモジュールの一例を示す概略図。

【図4】図3に示した有害情報遮断コードモジュールの動作を説明するフローチャート。

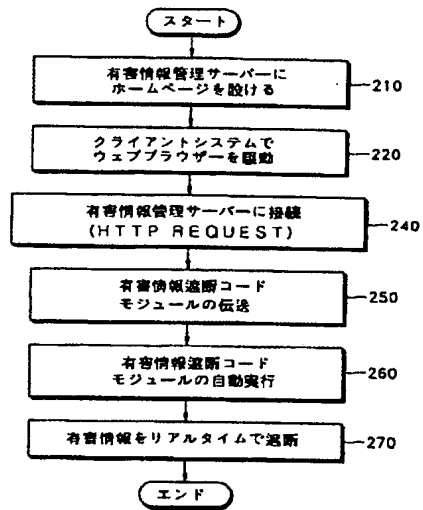
【図1a】



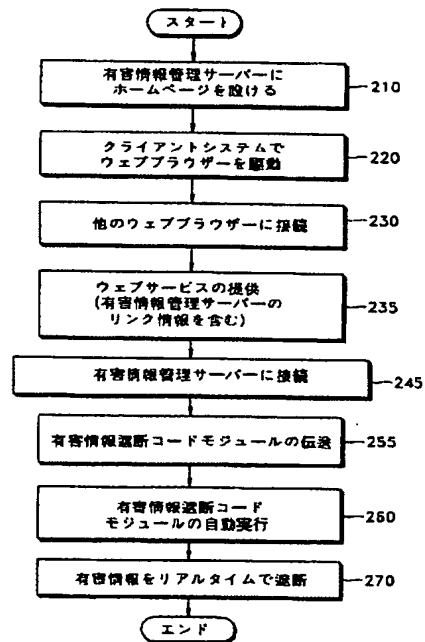
【図1b】



【図2a】



【図2b】



```

graph TD
    subgraph "コマンドモデルシステム"
        direction TB
        U1[入出力管理ユニット]
        U2[コマンド処理ユニット]
        U3[コマンド実行ユニット]
        U1 -- 310 --> U2
        U2 -- 320 --> U3
    end
    U2 --- S340[実行状態表示]
    S340 --- L340[340]
    L1[Fファイル/IO及びネットワーク  
パケット/Hooking] --> U1
    L2[コマンドの  
解析及び処理] --> U2
    L3[コマンド等に照するDATA  
をユーザーバーに伝送] --> U3

```

```

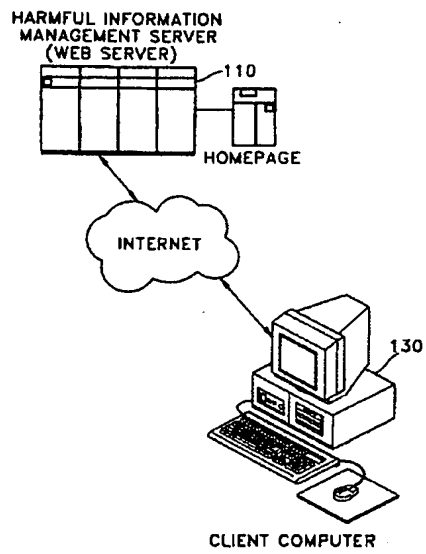
graph TD
    Start([スタート]) --> 410[実行中のプロセスの点検  
(有害プロセスの終了)]
    410 --> 420[FILE I/O  
(packet I/Oを含む) の  
監視 (hooking)]
    420 --> 430{使用中の情報が  
有害であるか?}
    430 -- いいえ --> 470[有害情報管理  
サーバーに通知]
    430 -- はい --> 440{FILE I/O  
であるか?}
    440 -- はい --> 450{治療可能であるか?}
    440 -- いいえ --> 460[通信ポートの遮断  
(実行中のプロセスの終了)]
    450 -- はい --> 454[治療]
    450 -- いいえ --> 452[実行を遮断]
    460 --> 462[流入した情報の治療]
    452 --> 470
    454 --> 470
    462 --> 470
    470 --> End([エンド])
  
```

WO 01/50344

PCT/KR00/01374

1/6

FIG. 1A

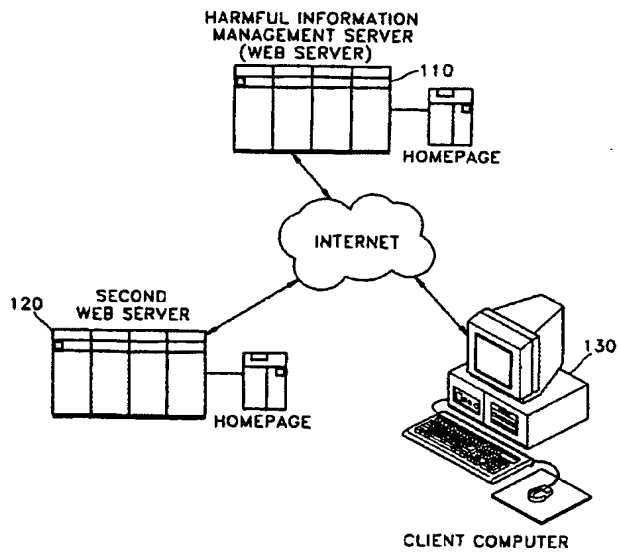


WO 01/50344

PCT/KR00/01374

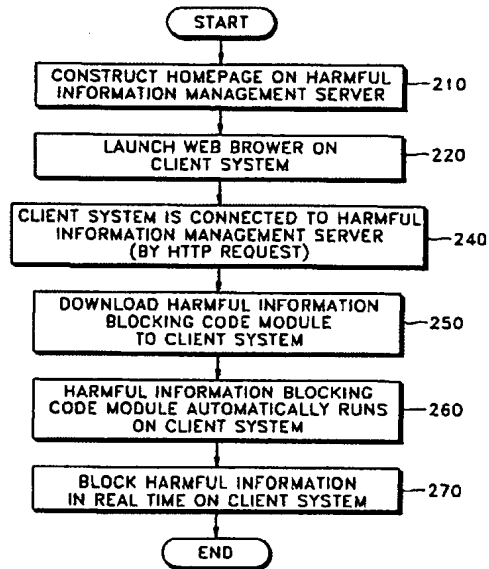
2/6

FIG. 1B



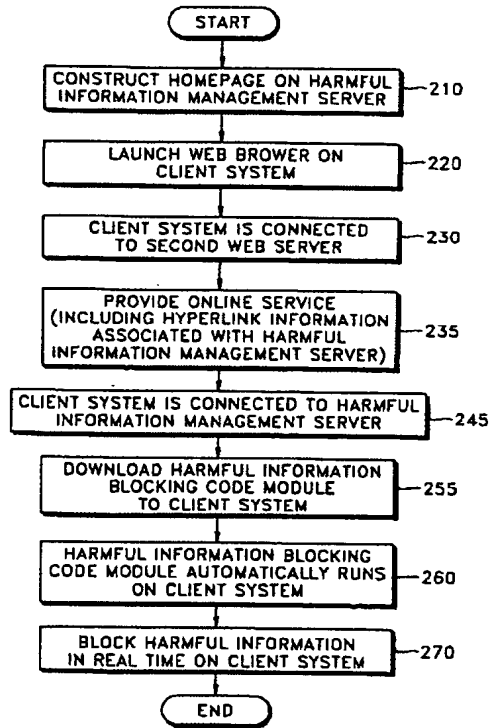
3/6

FIG. 2A



WQ 01/50344

PCT/KR00/01374

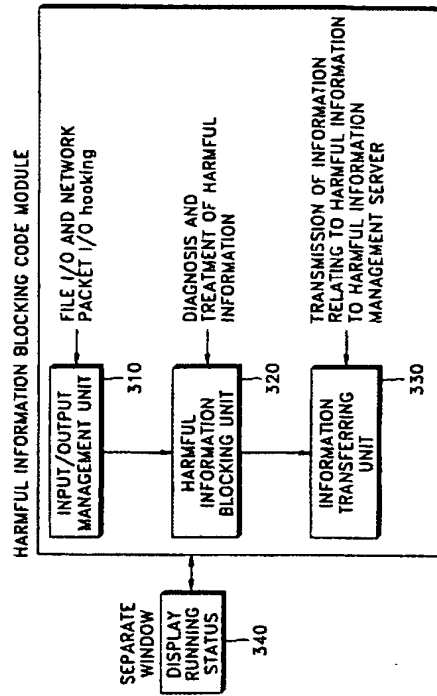
4/6
FIG. 2B

WO 01/50344

PCT/KR00/01374

5/6

FIG. 3

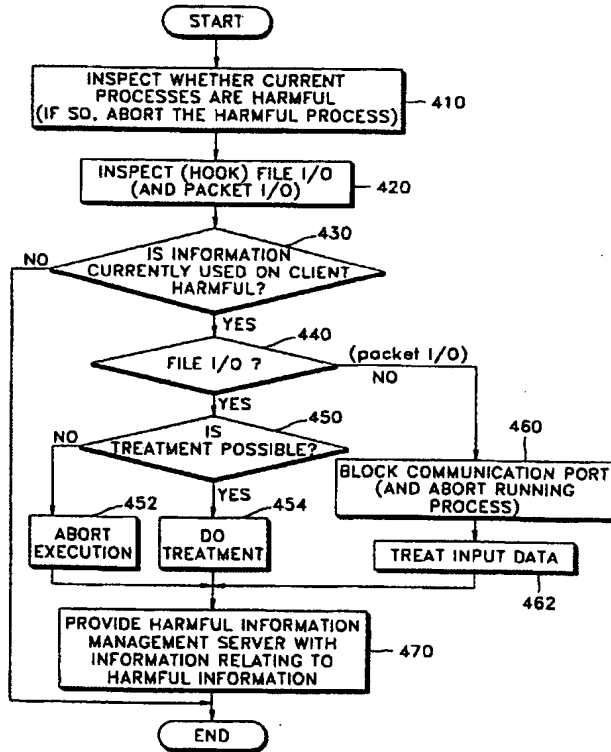


WO 01/56344


PCT/CR00/01374

6/6

FIG. 4



【国際調査報告】

INTERNATIONAL SEARCH REPORT		International Application No. PCT/KR00/01374
A. CLASSIFICATION OF SUBJECT MATTER IPC7 G06F 17/30 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC7 G06F 17/30 Documentation searched other than minimum documentation to the extent that such documents are included in the files searched KOREAN PATENTS AND APPLICATIONS FOR INVENTIONS SINCE 1975 KOREAN UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975 Electronic data base consulted during the International search (name of data base and, where practicable, search terms used) WPLPAI.WWW.DIGIATION.COM, "INFORMATION-AND-BLACK-AND-INTERNET-AND-CLIENT-AND-SERVER"		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US5706307 A (International Business Machines Corporation, Armonk, N.Y.) Jan 06, 1998 * Abstracts & claims	1, 13, 16, 23
Y	US6006034 A (Open Software Associates, Ltd., Kingwood, Australia) Dec. 21, 1999 * Abstracts & claims	1, 13, 16, 23
Y	US5790753 A (Digital Equipment Corporation, Maynard, Mass.) Aug. 04, 1998 * Abstracts & claims	1, 13, 16, 23
P,Y	US6049892 A (Ethos Software Corporation, Boston, Mass.) Apr. 11, 2000 * Abstracts & claims	1, 13, 16, 23
<input type="checkbox"/> Further documents are listed in the continuation of this C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "T" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of claims or other special reasons (as specified) "F" document referring to an oral disclosure, recitation, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "X" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "Y" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "W" document examiner of the same patent family		
Date of the actual completion of the international search 28 MARCH 2001 (28.03.2001)		Date of mailing of the international search report 29 MARCH 2001 (29.03.2001)
Name and mailing address of the ISA/KR Korean Industrial Property Office Government Complex, Taejeon, Daejeon-dong, Seok-su, Taejeon Metropolitan City 302-701, Republic of Korea Facsimile No. 82-42-472-7140 Form PCT/ISA/210 (second sheet) (July 1998)		Administrative office KIPI, Incheon Telephone No. 82-42-481-5786 

フロントページの続き

(81) 指定国 AP (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OA (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(特許庁注：以下のものは登録商標)

フロッピー

(72) 発明者 チョン、ヨンソプ

大韓民国 608-090 プサン ナムグ ヨンホードン 473-11 チンジュ グリー
ン ビラ 405

Fターム(参考) 5B076 AB20 BB06 FD08 FD09
5B089 KA17